

CLAIMS

What is claimed is:

- 1 1. A method for summarizing firewall activity, comprising:
 - 2 (a) organizing a plurality of types of events associated with a firewall of a local
3 computer;
 - 4 (b) tracking a number of occurrences of each type of event utilizing the firewall;
5 and
 - 6 (c) displaying a graphical representation indicating a severity of the number of
7 the events utilizing the firewall.
- 1 2. The method as recited in claim 1, wherein the events include blocked
2 attempts of various types.
- 1 3. The method as recited in claim 2, wherein at least one of the types of the
2 blocked attempts includes blocked attempts of remote computers to access
3 predetermined banned ports associated with the local computer.
- 1 4. The method as recited in claim 2, wherein at least one of the types of the
2 blocked attempts includes blocked attempts of remote computers with a
3 predetermined set of Internet Protocol (IP) addresses to access the local
4 computer.
- 1 5. The method as recited in claim 2, wherein at least one of the types of the
2 blocked attempts includes blocked attempts to access a network made by
3 predetermined applications.

- 1 6. The method as recited in claim 1, wherein the displayed number of
2 occurrences of each type of event occurred within a predetermined time
3 period.
- 1 7. The method as recited in claim 1, and further comprising displaying
2 additional information relating to the events upon the selection thereof.
- 1 8. The method as recited in claim 2, wherein a first type of the blocked attempts
2 includes blocked attempts of remote computers to access predetermined
3 banned ports associated with the local computer, a second type of the
4 blocked attempts includes blocked attempts of the remote computers with a
5 predetermined set of Internet Protocol (IP) addresses to access the local
6 computer, and a third type of the blocked attempts includes blocked attempts
7 to access a network made by predetermined applications.
- 1 9. The method as recited in claim 8, wherein the first type of the blocked
2 attempts, the second type of the blocked attempts, and the third type of the
3 blocked attempts are organized into categories.
- 1 10. The method as recited in claim 8, wherein a plurality of banned ports
2 associated with the first type of the blocked attempts are displayed with the
3 number of the occurrences associated therewith.
- 1 11. The method as recited in claim 8, wherein a plurality of banned IP addresses
2 associated with the second type of the blocked attempts are displayed with
3 the number of the occurrences associated therewith.
- 1 12. The method as recited in claim 8, wherein a plurality of banned applications
2 associated with the third type of the blocked attempts are displayed with the
3 number of the occurrences associated therewith.

20071586 020809

- 1 13. The method as recited in claim 8, and further comprising displaying a menu
2 for selecting from a summary page, an applications page, an event log, and
3 an IP address page.
- 1 14. The method as recited in claim 8, and further comprising displaying a menu.
- 1 15. The method as recited in claim 14, wherein upon the selection of an
2 applications page on the menu, displaying an applications interface for
3 selecting the predetermined applications.
- 1 16. The method as recited in claim 14, wherein upon the selection of an IP
2 address page on the menu, displaying an IP address interface for selecting the
3 predetermined IP addresses associated with the remote computers to be
4 blocked.
- 1 17. The method as recited in claim 14, wherein upon the selection of an event log
2 on the menu, displaying a log of the events.
- 1 18. The method as recited in claim 1, wherein the graphical representation
2 includes a bar graph.
- 1 19. A computer program product for summarizing firewall activity, comprising:
2 (a) computer code for organizing a plurality of types of events associated with a
3 firewall of a local computer;
4 (b) computer code for tracking a number of occurrences of each type of event
5 utilizing the firewall; and
6 (c) computer code for displaying a graphical representation indicating a severity
7 of the number of the events utilizing the firewall.
- 1 20. A system for summarizing firewall activity, comprising:

- 2 (a) logic for organizing a plurality of types of events associated with a firewall of
3 a local computer;
4 (b) logic for tracking a number of occurrences of each type of event utilizing the
5 firewall; and
6 (c) logic for displaying a graphical representation indicating a severity of the
7 number of the events utilizing the firewall.

- 1 21 A system for summarizing firewall activity, comprising:
2 (a) means for organizing a plurality of types of events associated with a firewall
3 of a local computer;
4 (b) means for tracking a number of occurrences of each type of event utilizing
5 the firewall; and
6 (c) means for displaying a graphical representation indicating a severity of the
7 number of the events utilizing the firewall.

- 1 22. A method for managing a firewall, comprising:
2 (a) displaying a menu for selecting from a summary page, an applications page,
3 and an Internet Protocol (IP) address page;
4 (b) upon the selection of the summary page on the menu, displaying a plurality
5 of types of blocked attempts, and an indication as to the number of
6 occurrences of each type of the blocked attempt, wherein a first type of the
7 blocked attempts includes blocked attempts of the remote computers with a
8 predetermined set of Internet Protocol (IP) addresses to access the local
9 computer, and a second type of the blocked attempts includes blocked
10 attempts to access a network made by predetermined applications;
11 (c) upon the selection of the applications page on the menu, displaying an
12 applications interface for selecting the predetermined applications; and
13 (d) upon the selection of the IP address page on a menu, displaying an IP address
14 interface for selecting the predetermined IP addresses associated with remote
15 computers to be blocked.

1 23. A method for managing a firewall and reporting firewall activity associated
2 therewith, comprising:
3 (a) displaying in a first portion of an event log a plurality of events;
4 (b) upon the selection of one of the events, displaying in a second portion of the
5 event log information relating to the event; and
6 (c) displaying a menu in a third portion of the event log a menu for selecting
7 from a summary page for summarizing the events, an application selection
8 page for selection of applications to be subject to security restrictions, and an
9 Internet Protocol (IP) address selection page for selection of IP addresses to
10 be subject to security restrictions.

1 24. A firewall method, comprising:
2 (a) executing a firewall in association with a local computer;
3 (b) identifying a number of blocked attempts of remote computers with a
4 predetermined set of Internet Protocol (IP) addresses to access the local
5 computer;
6 (c) identifying a number of attempts of the remote computers to access
7 predetermined frequently-used ports associated with the local computer;
8 (d) identifying a number of blocked attempts to access a network made by
9 predetermined applications on the local computer;
10 (e) displaying a menu for selecting from a plurality of interface features
11 including a summary page, an applications page, an event log, and an IP
12 address page;
13 (f) upon the selection of the summary page on the menu,
14 (i) displaying a recent activity list including recent activity icons
15 corresponding to events including total blocked attempts, the attempts
16 of the remote computers to access the predetermined frequently-used
17 ports associated with the local computer, the blocked attempts of the
18 remote computers with the predetermined set of IP addresses to
19 access the local computer, the recent activity list further including a
20 total number of the events within a predetermined time period

- 21 corresponding with each recent activity icon, and a graphical
22 representation indicating a severity of the total number of the events,
23 (ii) displaying a frequently accessed port list including port icons
24 corresponding to the predetermined frequently-used ports, the
25 frequently accessed port list further including a total number of the
26 attempts corresponding with each predetermined frequently-used
27 ports, and a graphical representation indicating a severity of the total
28 number of the attempts,
29 (iii) displaying a commonly blocked IP address list including IP address
30 icons corresponding to banned IP addresses from which the blocked
31 attempts of the remote computers occurred, the commonly blocked IP
32 address list further including a total number of the blocked attempts
33 corresponding with each IP address icon, and a graphical
34 representation indicating a severity of the total number of the blocked
35 attempts,
36 (iv) displaying a commonly blocked application list including application
37 icons corresponding to banned applications associated with the
38 blocked attempts, the commonly blocked application list further
39 including a total number of the blocked attempts corresponding with
40 each application icon, and a graphical representation indicating a
41 severity of the total number of the blocked attempts;
42 (g) upon the selection of the applications page on the menu, displaying an
43 applications interface for selecting the predetermined applications;
44 (h) upon the selection of the untrusted IP address page on the menu, displaying
45 an untrusted IP address interface for selecting the IP addresses associated
46 with remote computers to be blocked; and
47 (i) upon the selection of the event log on the menu, displaying a log of the
48 attempts.

10071586-020802
200820 0857:00T